



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,001	02/01/2002	Yaakov (Jordan) Levy	86120	2537
24628	7590	01/24/2006	EXAMINER	
WELSH & KATZ, LTD 120 S RIVERSIDE PLAZA 22ND FLOOR CHICAGO, IL 60606			HENNING, MATTHEW T	
			ART UNIT	PAPER NUMBER
			2131	
DATE MAILED: 01/24/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/062,001	Applicant(s) LEVY, YAAKOV (JORDAN)	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 November 2005.
 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-15 and 17 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1,3-15 and 17 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 01 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☒ All b) ☐ Some * c) ☐ None of:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2131

1 This action is in response to the communication filed on 11/10/2005.

2 **DETAILED ACTION**

3 *Response to Arguments*

4 Applicant's arguments regarding the prior art rejection of claims 1-3, 11, and 16, filed
5 11/10/2006 have been fully considered but they are not persuasive. The arguments merely recite
6 that claim 1 has been amended and therefore is deemed allowable. These arguments have not
7 been found persuasive.

8 However, based on the reasons presented below, the previous prior art rejections have
9 been withdrawn.

10 The examiner notes the applicant's argument on page 9 in paragraph 9 which attempts to
11 claim that one of ordinary skill in the art would understand the scope of the relative term "close"
12 as it is used in claim 1. However, in the argument the applicant has attempted to show that
13 "close" means differing by no more than a "small" integer or differing in size by no more than a
14 "few" bits. Both of "small" and "few" are also relative terms which only lessen the clarity of the
15 scope of "close". As such, the examiner has not found this explanation persuasive as to the
16 clarity of the claim language and has acted accordingly below.

17 Regarding the applicant's argument that the rejection of claims 1-16 under 35 USC 101
18 was improper, the examiner does not find the argument persuasive. These claims consist solely
19 of mathematical operations without some claimed practical application.

20 A claim that requires one or more acts to be performed defines a
21 process. However, not all processes are statutory under **35 U.S.C. 101**.
22 *Schrader*, 22 F.3d at 296, 30 USPQ2d at 1460. To be statutory, a claimed
23 computer-related process must either: (A) result in a physical
24 transformation outside the computer for which a practical application in the
25 technological arts is either disclosed in the specification or would have

Art Unit: 2131

1 been known to a skilled artisan (discussed in i) below), or (B) be limited to
2 a practical application within the technological arts (discussed in ii) below).
3 See *Diamond v. Diehr*, 450 U.S. at 183-84, 209 USPQ at 6 (quoting
4 *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1877)) ("A [statutory] process
5 is a mode of treatment of certain materials to produce a given result. It is
6 an act, or a series of acts, performed upon the subject-matter to be
7 transformed and reduced to a different state or thing.... The process
8 requires that certain things should be done with certain substances, and in
9 a certain order; but the tools to be used in doing this may be of secondary
10 consequence."). See also *Alappat*, 33 F.3d at 1543, 31 USPQ2d at 1556-
11 57 (quoting *Diamond v. Diehr*, 450 U.S. at 192, 209 USPQ at 10). See
12 also *id.* at 1569, 31 USPQ2d at 1578-79 (Newman, J., concurring)
13 ("unpatentability of the principle does not defeat patentability of its
14 practical applications") (citing *O'Reilly v. Morse*, 56 U.S. (15 How.) at 114-
15 19). If a physical transformation occurs outside the computer, a disclosure
16 that permits a skilled artisan to practice the claimed invention, i.e., to put it
17 to a practical use, is sufficient. On the other hand, it is necessary for the
18 claimed invention taken as a whole to produce a practical application if
19 there is only a transformation of signals or data inside a computer or if a
20 process merely manipulates concepts or converts one set of numbers into
21 another.

22 A process that merely manipulates an abstract idea or performs a purely
23 mathematical algorithm is nonstatutory despite the fact that it might
24 inherently have some usefulness. In *Sarkar*, 588 F.2d at 1335, 200 USPQ
25 at 139, the court explained why this approach must be followed:

26 No mathematical equation can be used, as a practical matter, without
27 establishing and substituting values for the variables expressed therein.
28 Substitution of values dictated by the formula has thus been viewed as a
29 form of mathematical step. If the steps of gathering and substituting values
30 were alone sufficient, every mathematical equation, formula, or algorithm
31 having any practical use would be per se subject to patenting as a
32 "process" under **101**. Consideration of whether the substitution of specific
33 values is enough to convert the disembodied ideas present in the formula
34 into an embodiment of those ideas, or into an application of the formula, is
35 foreclosed by the current state of the law.

36 For such subject matter to be statutory, the claimed process must be
37 limited to a practical application of the abstract idea or mathematical
38 algorithm in the technological arts. See *Alappat*, 33 F.3d at 1543,
39 31 USPQ2d at 1556-57 (quoting *Diamond v. Diehr*, 450 U.S. at 192, 209
40 USPQ at 10). See also *Alappat* 33 F.3d at 1569, 31 USPQ2d at 1578-79
41 (Newman, J., concurring) ("unpatentability of the principle does not defeat
42 patentability of its practical applications") (citing *O'Reilly v. Morse*, 56 U.S.

Art Unit: 2131

(15 How.) at 114-19). A claim is limited to a practical application when the method, as claimed, produces a concrete, tangible and useful result; i.e., the method recites a step or act of producing something that is concrete, tangible and useful. See *AT&T*, 172 F.3d at 1358, 50 USPQ2d at 1452. Likewise, a machine claim is statutory when the machine, as claimed, produces a concrete, tangible and useful result (as in *State Street*, 149 F.3d at 1373, 47 USPQ2d at 1601) and/or when a specific machine is being claimed (as in *Alappat*, 33 F.3d at 1544, 31 USPQ2d at 1557 (*en banc*)). For example, a computer process that simply calculates a mathematical algorithm that models noise is nonstatutory. However, a claimed process for digitally filtering noise employing the mathematical algorithm is statutory.

See MPEP § 2106.IV.1

As such, because the method is simply manipulating data, it is non-statutory. Further, simply because the data is being manipulated in a "computation device" does not make the claim statutory. As such, the examiner has maintained the rejections under 35 USC 101.

Regarding the amendment to the Abstract, the Abstract as amended still does not meet the length requirement of 50 words and therefore the objection to the specification has been maintained below.

Claims 1, 3-15, and 17 have been examined.

All objections and rejections not presented below have been withdrawn.

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because:

The abstract is objected to for failing to meet the length requirement of 50 words.

Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 3-15 and 17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-15 and 17 are directed towards a method for simply manipulating data, and as discussed above with in the response to arguments section, they are non-statutory.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 3-15, and 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "close" in claim 1 is a relative term which renders the claim indefinite. The term "close" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Although the specification and the remarks provided in the communication dated 11/10/2005 attempt to clarify what is meant by the term "close",

Art Unit: 2131

1 clarification has not been achieved. This is due to the fact that the specification and remarks use
2 other relative terms (i.e. few and small) to establish some meaning to the term “close”. One of
3 ordinary skill in the art would be unable to determine the scope of “a few bits” as this could be
4 interpreted to mean 3 bits, 4 bits, or even possibly 25 or more bits if we are comparing 100,000
5 bits. Further, one of ordinary skill in the art would be unable to determine the scope of “a small
6 integer”. This could be interpreted anywhere from 0 to ∞ depending on the size of the numbers
7 being compared. For instance, if the numbers being compared are on the order of ∞^2 then a
8 difference between the two of ∞ might be considered small. As such, the use of the term “close”
9 in the claims has rendered the scope of the claims indeterminate. Therefore, claims 1-15 and 17
10 are rejected for failing to particularly point out and distinctly claim the subject matter which the
11 applicant regards as the invention.

12 Claims 3 recite the limitation "gcd(a, b)". There is insufficient antecedent basis for this
13 limitation in the claim. Furthermore it is unclear from the specification what the function gcd(a,
14 b) represents. Although in mathematics it represents the “greatest common divisor” of the
15 variables ‘a’ and ‘b’, it has not been specifically pointed out that this is the case in the present
16 application. As such, the scope of the claim is not clearly defined. The examiner will permit an
17 amendment to the specification in order to clarify that gcd(a, b) represents the “greatest common
18 divisor” of the variables ‘a’ and ‘b’. If in fact, this is not the case and gcd(a, b) is meant to
19 represent some other function, the amendment will not be entered as this would constitute new
20 matter.

21 Claims 4-15 and 17 are rejected by virtue of their dependency to claims 1 and 3.

22

Art Unit: 2131

Allowable Subject Matter

Claims 1, 3-15, and 17 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, and 35 USC 101 set forth in this Office action.

The following is a statement of reasons for the indication of potentially allowable subject matter:

The prior art fails to teach or suggest a combination as claimed in independent claim 1, including providing two numbers u and v such that the sum of u and v is close to n , u is greater than $n/2$, and v is neither close to 0 nor close to n , where n is the number of bits in a modulus N .

Ong et al. (An Efficient Signature Scheme Based on Quadratic Equations) disclosed providing a modulus N ; providing a number V in the ring Z_N , wherein for another number S in the ring Z_N , $V \cdot S^2 = 1$ in Z_N ; solving an equation in Z_N to provide x and y ; and assigning SIG as the signature of the message, wherein SIG comprises (x, y, z) . However, Ong et al. does not teach or suggest a combination as claimed in independent claim 1 including providing a message digest to sign instead of the message itself, or solving the equation: $(M_x + x)^2 - V \cdot y^2 = 4(M_z + z)$ for x , y , and z , or providing two numbers u and v such that the sum of u and v is close to n , u is greater than $n/2$, and v is neither close to 0 nor close to n , where n is the number of bits in a modulus N . Therefore, claims 1, 3-15, and 17 are potentially allowable over Ong et al.

Okamoto et al. ("An Efficient Digital Signature Scheme Based on an Elliptical Curve Over the Ring Z_N ") disclosed a signature scheme based on Elliptic curve over Z_N involving a multiple variable signature wherein the signing is performed on the message digest (m_x, m_y) of the message. Okamoto et al. further teaches that a signature can be composed of multiple variables and the signature is formed by solving a one way multivariable formula for the

Art Unit: 2131

variables. However, Okamoto et al. does not teach or suggest a combination as claimed in independent claim 1, including solving the specific equation: $(M_x + x)^2 - V \cdot y^2 = 4(M_z + z)$ for x , y , and z , or providing two numbers u and v such that the sum of u and v is close to n , u is greater than $n/2$, and v is neither close to 0 nor close to n , where n is the number of bits in a modulus N .

Therefore, claims 1, 3-15, and 17 are potentially allowable over Okamoto et al.

Conclusion

Claims 1, 3-15, and 17 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew Henning
Assistant Examiner
Art Unit 2131
1/19/2006



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100